

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2002年1月3日 (03.01.2002)

PCT

(10) 国際公開番号
WO 02/01533 A1

(51) 国際特許分類: G08G 1/137, H04M 11/00, 3/42, G06F 13/00, 17/60

(52) 国際出願番号: PCT/JP01/05664

(53) 国際出願日: 2001年6月29日 (29.06.2001)

(54) 国際出願の言語: 日本語

(55) 国際公開の言語: 日本語

(56) 優先権データ:
特願2000-201462 2000年6月29日 (29.06.2000) JP
特願2001-188724 2001年6月21日 (21.06.2001) JP

(57) 出願人(米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人(米国についてのみ): 池田清和 (IKEEDA, Kiyokazu) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 弁理士 松隈秀盛 (MATSKUMA, Hiromori); 〒160-0023 東京都新宿区西新宿1丁目8番1号 新宿ビル Tokyo (JP).

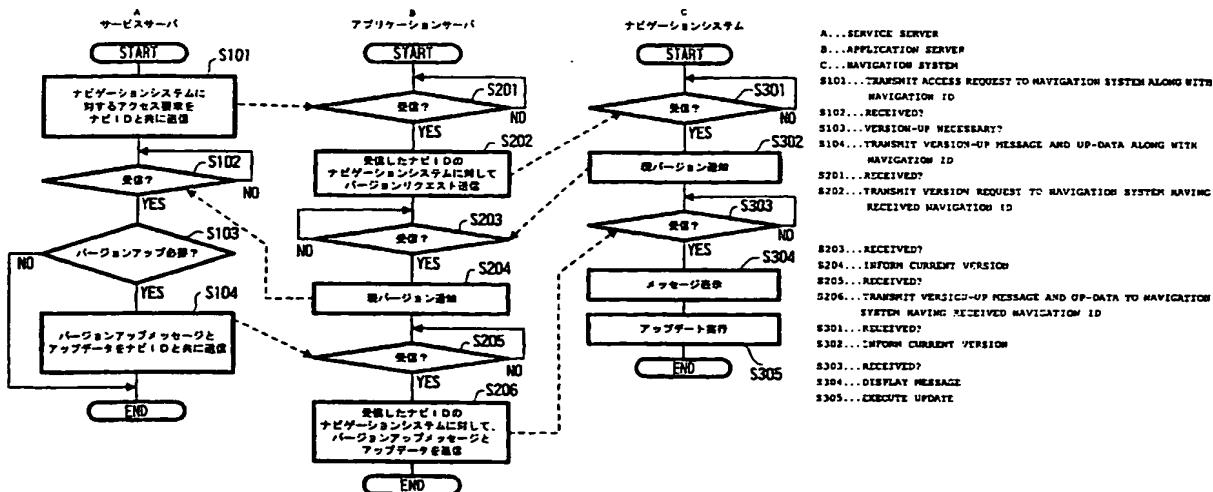
(81) 指定国(国内): CN, DE, US.

添付公開書類:
— 國際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイドスノート」を参照。

(54) Title: SERVICE PROVIDING SYSTEM

(54) 発明の名称: サービス提供システム



WO 02/01533 A1

(57) Abstract: A service server for providing service which uses, in order to improve after service for products purchased by users, an apparatus ID specifically allocated to a navigation system, a product purchased by a user, to access a specific navigation system and transmit navigation information. Namely, it positively accesses a navigation system that is one of an unspecified number of terminal devices on a communication network to transmit and provide service information, whereby it is possible to provide service having necessary and sufficient contents at any proper opportunity.

/統葉有/

明細書

サービス提供システム

技術分野

本発明は、例えば自動車などの移動体に搭載される電子機器と
5 、サーバ及び携帯電話などの個人移動端末装置とを通信網を介して通信可能なように構築されたシステムとして、例えば電子機器を購入して利用しているユーザに対して、送信されたデータを受信した電子機器が、その受信データの内容に従って何らかの動作の実行を行うことで享受できるようなサービスを提供することの
10 できるシステムに関するものである。

背景技術

いわゆるカーナビゲーション装置が広く普及している。その基本的な機能としては、例えば移動中にある自動車などの現在位置を測定して、その測定された現在位置を地図上に表示させるなどして、ユーザに現在位置を知らせるものである。

また、近年においては、移動無線端末装置を備えることで、インターネットに接続可能な機能を有するカーナビゲーション装置も普及してきている。その利用形態としては、例えばインターネット上のWebサイトにアクセスすることで、例えば、或る特定地域の店舗の情報や、イベント、天気の情報などをカーナビゲーション装置の表示部位に表示させ、これらの情報を得ることが可能になるものである。

ところで、例えば商品を購入したユーザには、いわゆるアフターケア、アフターサービスなどといわれる、商品を購入したユーザにとって有用となるようなサービスを、その商品を製造販売したメーカーや店舗から提供することがしばしば行われる。

ここで上記したようなカーナビゲーション装置もまた、元は商

テムについて以下のように構成する。

本発明のサービス提供システムは、少なくとも、無線通信端末機能を備えて移動体に搭載されると共に、固有となる機器 ID が割り与えられる電子機器と、所定のサービス提供機能を有すると共に、サービス提供可能な複数の上記電子機器についての上記機器 ID が格納されるサービス用サーバと、通信網とを備えて成る。

そして、上記サービス用サーバからサービス提供が必要とされる特定の電子機器に対して、機器 ID を利用して通信網を介してアクセスし、アクセスした電子機器に対して、特定のサービスを実現するための所定内容を有するサービス情報を送信するための送信手段を備えることとした。

また、少なくとも、無線通信端末機能を備えて移動体に搭載されると共に、固有となる機器 ID が割り与えられる電子機器と、所定のサービス提供機能を有すると共に、サービス提供可能な複数の上記電子機器についての上記機器 ID が格納されるサービス用サーバと、通信網とを備えて成るサービス提供システムとして、電子機器からサービス用サーバに対して通信網を介してアクセスし、特定のサービスに利用可能な所定内容の情報を送信することができる第 1 の通信手段と、サービス用サーバからサービス提供が必要とされる特定の電子機器に対して、機器 ID を利用して通信網を介してアクセスし、アクセスした電子機器に対して、特定のサービス提供を実現するための所定内容を有するサービス情報を送信するための第 2 の通信手段とを備えることとした。

また、少なくとも、無線通信端末機能を備えて移動体に搭載されると共に、固有となる機器 ID が割り与えられる電子機器と、固有となる端末 ID が割り与えられる移動無線端末装置と、通信網とを備えて成るサービス提供システムとして、移動無線端末装

網に接続される認証サーバとから成るものとされる。

そして、通信端末装置が、電子機器に固有となるように割り与えられる機器 ID を利用して通信網を介して電子機器にアクセスするのに、認証サーバを経由してのみ上記電子機器にアクセスすることを可能とするアクセス手段と、通信網内において、通信端末装置が通信網に対してアクセスしてきたアクセス経路を特定する情報をを利用して、通信端末装置の端末 ID を生成する端末 ID 生成手段と、認証サーバにおいて、端末 ID を利用して、アクセスしてきた通信端末装置についての認証処理を行うとともに、認証が成立した場合にのみ、通信端末装置が電子機器に対してアクセスすることを許可する認証対応処理手段と、認証対応処理手段によってアクセスが許可された通信端末装置と電子機器との間において、通信網を介して特定のサービス提供を実現するための所定内容を有するサービス情報の送受信が行われるようにする送受信手段とを備えることとした。

上記構成においては、例えば家庭内や企業などではほぼ固定的に設置されることで、通信網までのアクセス経路も固定されるような通信端末装置と、移動体に搭載されたり、携帯されることで移動することが想定される電子機器と通信を行うのにあたっては、通信端末装置が、相手側の電子機器の機器 ID を利用してアクセスするようになる。そして、アクセス後におけるサービス情報の送受信によって特定のサービス提供が実現されることになる。

つまりは、この構成によっても、本来は通信網上において不特定多数の端末装置の 1 つである電子機器に対して積極的にアクセスして通信を行うことでサービスを提供することが可能とされるものである。

そのうえで、上記構成においては、通信端末装置から電子機器へのアクセスにあたって認証サーバが介在することになる。そし

示すブロック図である。

図7は、システムバージョンアップのサービス提供を実現するための処理動作を示すフローチャートである。

5 図8は、自動車のセキュリティチェックを携帯電話から行うというサービス提供を実現するための処理動作を示すフローチャートである。

図9は、自動車の鍵を、携帯電話からのコントロールにより行うというサービス提供を実現するための処理動作を示すフローチャートである。

10 図10は、地図情報の更新データをナビゲーションシステムがサービスサーバからダウンロードするというサービスを実現するための処理動作を示すフローチャートである。

図11は、本発明の実施の形態としてのサービス提供システム(第2例)の構成例を示す説明図である。

15 図12は、パーソナルコンピュータの内部構成例を示すブロック図である。

図13は、本実施の形態における認証サーバの内部構成例を示すブロック図である。

20 図14は、本実施の形態におけるPC-ID登録手順(第1例)を示す概念図である。

図15は、本実施の形態におけるPC-ID登録手順(第2例)を示す概念図である。

図16は、本実施の形態におけるPC-ID登録手順(第3例)を示す概念図である。

25 図17は、パーソナルコンピュータがナビゲーションシステムの現在位置情報を取得するというサービスを実現するための処理動作を示すフローチャートである。

図1は、本実施の形態の第1例としてのサービス提供システムの一形態例を示している。

自動車100には、ナビゲーションシステム1が搭載されている。このナビゲーションシステムは、いわゆるカーナビゲーション装置を基本として、自動車の盗難などを防ぐセキュリティシステム、また、無線電話通信網300を介してデータ通信が可能な通信端末装置などを備えたシステム構成を探っている。

本実施の形態のサービス提供システムによるサービスを受けるのは、この自動車100の所有者であり、また、ナビゲーションシステム1を購入したユーザとなる。

携帯電話200は、例えばナビゲーションシステムと同じユーザの名義で、無線電話通信網300を運営する通信会社と契約してあるもので、上記のようにして、無線電話通信網300を介して、電話回線を使用しての通話を行うことができる。また、この場合には、インターネットとの接続によりデータ通信を行うことも可能とされている。

無線電話通信網300は、例えば携帯電話のほか、本実施の形態であればカーナビゲーション装置の無線端末装置などの、無線端末装置間の移動体通信を実現するための設備とされ、例えば図示するように、基地局301、中継局302、アプリケーションサーバ303、ゲートウェイ304を備える。

基地局301及び中継局302によっては、例えば無線端末装置間での無線通信が可能とされる。また、無線端末装置をインターネットと接続する際には、アプリケーションサーバ303がその機能を果たすようにされる。

アプリケーションサーバ303は、例えばその無線通信会社で提供するインターネット機能に対応して必要となる処理を実行するようにされている。そして、アプリケーションサーバ303に

を示している。

この図2に示す本実施の形態のナビゲーションシステム1は、
例えはナビゲーション本体部2、ディスプレイモニタ部3、G P
Sアンテナ5、交通情報受信アンテナ7、自律航法ユニット6、
5 通信端末装置50、セキュリティシステム部41、及びリモート
コントローラ8等によって構成される。

ナビゲーション本体部2の詳しい構成については後述するが、
その内部で再生される記録媒体9から読み出した地図情報と、現在
10 位置情報とに基づいて、例えはディスプレイモニタ部3の表示
画面3aに対して、自車の現在位置を地図上に表示させたり、また、
ドライブ経路や各種ガイドとなるナビゲーション情報を表示
させることができるようになっている。

記録媒体9は、例えはこの場合には、C D - R O M (Compact
Disk - Read Only Memory) や、D V D - R O M (Digital Video
15 Disk / Digital Versatile Disk - Read Only Memory) 等のディスク
とされ、上記もしたように地図情報が記憶されている。

ディスプレイモニタ部3の表示画面部3aには、例えは液晶ディスプレイ等によって構成され、ナビゲーション本体部2から出力される画像情報に基づいて表示が行われる。

受信部3bはリモートコントローラ8から送られてくるコマンド情報を受信する受信部とされる。この受信情報は、後述するよ
うにして、ナビゲーション本体部2に対して伝送される。

また、ここでは図示していないが、本実施の形態のナビゲーション装置としては、スピーカ等の音声出力部を設けることも可能とされる。その場合は、ナビゲーション本体部2から音声出力部に対して、所定のポイント(交差点)や、渋滞状況、右折左折地点、道順間違い、などといった音声ナビゲーション情報を出力することで、音声出力部からユーザに対して警告音やガイド音声を

、コマンド信号を赤外線輝度変調信号として出力する出力部等を備えており、その赤外線によるコマンド出力が上記受信部 3 b で受信される。

ここで、リモートコントローラ 8 に備えられる緊急キー 8 a は
5 、例えば交通事故や、第三者とのトラブルなどの、搭乗者にとって危険とされる状況が発生したときに操作されるもので、これによって、例えば、そのときの状況を記録した画像、音声データを転送させることができるようになっている。

なお、操作手段としては、これ以外にも、例えば電波送信によるリモートコントローラ、ナビゲーション本体部 2 と有線接続されるリモートコントローラ、さらにはナビゲーション本体部 2 やディスプレイモニタ部 3 の筐体上に設けられる操作部等とされてもよいものである。
10

通信端末装置 5 0 は、先に図 1 に示した無線電話通信網 3 0 0 を介するようにしてインターネットに接続するための移動体通信端末である。そして、この通信端末装置 5 0 は、図示するようにナビゲーション本体部 2 と接続されることで、ナビゲーション本体部 2 からデータを無線によって送信することが可能となり、また、通信端末装置 5 0 にて受信したデータを入力して、ナビゲーション本体部 2 にて所要の処理を実行することが可能となるものである。つまり、通信端末装置 5 0 とナビゲーション本体部 2 とが接続されることで、本実施の形態のナビゲーションシステム 1 には、少なくともインターネット接続機能が与えられる。
15
20

セキュリティシステム部 4 1 は、自動車自体及び搭乗者を保安するための機能を有するものとされ、この場合には、外付けカメラ 4 2 、マイクロフォン 4 3 、ロックコントロール部 4 4 、及び記憶部 4 5 を備えてなる。
25

外付けカメラ 4 2 は、例えば実際には、複数のカメラ装置から

タとして記憶部45への記録が行われる。

ロックコントロール部44は、自動車の鍵の開閉動作をコントロール可能なように自動車への取り付けが行われる。また、鍵の開閉をコントロール機構部位の状態に応じて、現在、鍵がかかっているか否かを示すロック状態情報をナビゲーション本体部2に対して出力することも可能になっている。

記憶部45は、例えば比較的大容量のデータを記憶可能な記憶デバイスを備えて成る。ここでは、この記憶部45として採用されるメディアは特に限定はしないが、例えばハードディスクであってもよいし、また、他のディスクメディアや不揮発性のメモリ素子などが採用されて構わない。本実施の形態の場合には、記憶部45には、上記した各カメラ装置に撮像された動画像データ、及び、マイクロフォン43により収音された音声信号データが、自動車内部及び周囲の状況を再現する証拠的な情報として記憶される。

1-3. ナビゲーション本体部の内部構成

図3のブロック図は、ナビゲーション本体部2の内部構成を示している。

この図4において、測位部4は自車の現在位置を測位する部位であり、インターフェイス14から転送されてくるG P Sの受信データや、自車の走行情報に基づいて例えば所定の演算処理を実行することで、自車の現在位置を示す位置情報としての緯度／経度情報を得るようにされる。

R O M (Read Only Memory) 11には、本実施の形態のナビゲーションシステム1が所要の処理を実行するための各種プログラム、及び原則として書き換え不可の各種ファクトリープリセット

ション本体部 2 とを接続するために設けられる。

この場合のインターフェイス 1 4 には、G P S アンテナ 5 からの受信データが入力される。また、交通情報アンテナ 7 にて受信された道路交通情報のデータが入力される。自律航法ユニット 6 の車速センサにて検出される車速パルスが入力される。また端子 3 2 を介しては、ジャイロ 6 b にて検出される自車の走行方向情報が入力される。

10 G P S アンテナ 5 からの受信データと、自律航法ユニット 6 からの走行情報（車速パルス及び走行方向情報）は、バス 2 0 を介して測位部 4 に転送される。測位部 4 では、これらの転送された情報をパラメータとして入力して、自車の現在位置を測定する。

15 また、交通情報アンテナ 7 からの道路交通情報のデータは、例えば制御部 1 9 の制御によってD R A M 1 3 に書き込まれて保持されると共に、制御部 1 9 がこのD R A M 1 3 に書き込んだ道路交通情報を参照することで、例えばディスプレイモニタ部 3 に対して表示出力すべき地図情報画像データにおいて渋滞状況等の道路交通情報が反映されるようにも画像処理制御等を実行するよう にされる。

20 時計部 1 5 は、現在日時を計時するもので、その時間情報は、当該ナビゲーションシステム 1 において必要とされる時間管理のために用いられる。

25 入力部 1 6 は、ディスプレイモニタ部 3 の受信部 3 b と接続されており、受信部 3 b で受信したリモートコントローラ 8 からのコマンド信号が入力される。そして、入力されたコマンド信号を内部バス 2 0 により伝送可能なフォーマットに変換した後、バス 2 0 を介して制御部 1 9 に転送する。制御部 1 9 では、入力したコマンド信号に基づいて適宜所要の制御処理を実行するよう にされる。

が行われる。

また、記憶部 4 5 に対して動画像データ及び音声データを記録するのにあたっては、例えば記録を行っていく過程で、記録可能容量が一杯になったときには、最も過去に記録された動画像データ及び音声データを上書き消去していくようにして、最新の撮像画像データ及び音声データを記録していくようにされる。このようにすれば、記憶部 4 5 の記憶容量としては比較的少なくとも済む。この記録可能容量としては時間的に例えば数 10 分程度であれば、証拠を残すという目的には充分に適うものとされる。

なお、上記画像音声処理部 4 6 としては、例えば、記憶部 4 5 に記録された画像音声データを再生出力するためのデコード機能を備えるようにしても構わない。このようなデコード機能を与えれば、例えば記憶部 4 5 に記録された画像音声データを表示部 3 にて再生出力させることも可能とされる。

通信インターフェイス 4 7 は、通信端末装置 5 0 とナビゲーション本体部 2 との間でのデータの送受信を司る。例えば通信端末装置 5 0 からナビゲーション本体部 2 側にデータ出力が行われた場合には、通信インターフェイス 4 7 は、通信端末装置 5 0 から入力されたデータを、ナビゲーション本体部 2 内で処理可能な形式に変換して、データバス 2 0 を介して所要の機能回路部に出力する。

また逆に、ナビゲーション本体部 2 から通信端末装置 5 0 に対してデータを転送する場合には、通信端末装置 5 0 により処理可能な形式のデータに変換して通信端末装置 5 0 に対して出力するようになる。

またここでは、通信端末装置 5 0 に対する動作制御は、ナビゲーション本体部 2 の制御部 1 9 が実行するようになる。つまり、通信端末装置 5 0 とナビゲーション本体部 2 とが連携して無線

て入力される。信号処理回路 204 では、この音声信号について所定のエンコード処理を施して送信回路 203 に対して出力する。送信回路 203 では、信号処理回路 204 から入力された信号をアンテナ 1 を介して送信出力させる。

5 システムコントローラ 208 は、当該携帯電話による各種動作が行われるように各種制御処理を実行する。

10 このシステムコントローラ 208 には、ROM 217 及び RAM 218 が備えられる。ROM 217 は、例えばフラッシュメモリや EEPROM などにより構成される書き換え可能なメモリとされ、ここにシステムコントローラ 208 が実行すべきプログラムや表示データが記憶される。また、例えば電話帳データや、送受信したメールのデータなど、ユーザが設定、登録した各種データも記憶保持される。

15 更に本実施の形態においては、ROM 217 には、この携帯電話 200 に対して固有に与えられた携帯 ID が付される。これは、携帯電話の場合であれば、割与えられた電話番号の情報としてもよいものである。

20 キー操作部 210 は、所定複数のボタンキーから成るものとされ、これらボタンキーに対する操作に応じた操作情報信号をシステムコントローラ 208 に対して出力する。システムコントローラ 208 は、この操作情報信号に基づいて、所要の動作が得られるように制御処理を実行する。

25 また、LCD 表示部 209 は、図示するように、システムコントローラ 208 の制御によって、動作状況に応じた内容の表示が行われるように駆動される。

なお、ナビゲーションシステム 1 に備えられる通信端末装置 50 の内部構成も、上記図 4 に示す構成に準じたものとされる。但し、通信端末装置 50 の場合には、これをユーザが携帯して通話

、ユーザが所有するナビゲーションシステム1に割与えられたものと同一のナビIDのデータが格納される。なお、このナビIDとしては、例えば無線端末装置50に対して割り与えた電話番号とすることが考えられ、ナビIDを電話番号とすれば、例えばアプリケーションサーバ303、またはサービスサーバ500から、ナビゲーションシステム1の無線端末装置にアクセスすることを容易に実現できる。

また、例えば携帯電話200から、無線電話通信網300を介するようにしてナビゲーションシステム1に対してアクセスする場合には、アクセスを要求した携帯電話200が適正であることの認証を得るために、携帯電話200に対してユーザがパスワードの入力操作を行うのであるが、ユーザデータベース410のパスワードとしては、この値が格納されることになる。

ところで、図5に示されるユーザデータベース410の内容として、各ユーザ個人ごとの情報は、例えば次のような機会において、所要の情報を取得して作成することができる。

例えばナビゲーションシステム1は、インターネットを利用したいわゆるインターネットショッピングにより購入することができるものとしている。このようなインターネットショッピングにより購入手続きを行うのにあたっては、例えばユーザは、ブラウザ画面上に表示される入力フォームに対して所要の個人情報を入力する。また、本実施の形態のようにして無線端末装置50を備えるナビゲーションシステム1であれば、このナビゲーションシステム1の購入に際して、無線端末装置50を利用可能とするための通信会社との契約も行うようになれる。本実施の形態では、アプリケーションサーバ303（またはサービスサーバ500）が、インターネットショッピングのための販社サーバと通信することで、これらの情報を受け取り、そしてデータベースとして作

アクセス要求に応じてのインターネットとの接続処理や、ユーザデータベース 410 を検索するためのアプリケーションプログラムなどである。

インターフェイス 402 は、中継局 302 側との情報送受信のために設けられ、インターフェイス 403 は、ゲートウェイ 304 (インターネット) 側との情報送受信のために設けられる。

制御部 404 は、実行アプリケーション 411 としてのプログラム内容に従って各種の制御処理を実行する。

10 1 - 6. サービスサーバの内部構成

図 6 は、サービスサーバ 500 の内部構成例を簡略に示している。

この図に示すサービスサーバ 500 は、記憶部 501、ネットワークインターフェイス 502、制御部 503 を備える。

この場合にも記憶部 501 には、各種サービスを提供するサーバとしての機能を実現するのに必要とされる各種情報が記憶されている。ここでは、記憶部 501 に格納される代表的なデータとして、ユーザデータベース 510、実行アプリケーション 511、サービス用データ 512 が示される。

ユーザデータベース 510 は、例えば先に図 5 において説明したユーザデータベース 410 と同様の内容でよいものとされ、例えば、アプリケーションサーバ 303 と通信を行うことで、常に同じ内容を保有しているようにされる。つまり、アプリケーションサーバ 303 またはサービスサーバ 500 との何れか一方のサーバにおいて、ユーザの新規契約などによってユーザデータベースの内容が更新されると、他方のサーバに対してユーザデータベースが更新されたことを通知して、互いのユーザデータベースの

ナビ I D と共に、サービス用データ 512 として最新版のメディアを勧めるコンテンツデータを、無線電話通信網 300 のアプリケーションサーバ 303 に対して送信する。このコンテンツデータは、例えば「地図ディスクの新盤がでています。もしよろしければお買い求め下さい。入手方法は・・・」などのような文字を、表示部 3 の表示画面 3a に表示出力可能なデータとされる。

5 アプリケーションサーバ 303 では、ユーザ I D とコンテンツデータを受信すると、受信したユーザ I D のナビゲーションシステム 1 のすべてに対してコンテンツデータを送信する。

10 そして、このコンテンツデータは、ナビゲーションシステム 1 の無線端末装置 50 にて受信されてナビゲーション本体部 2 に対して転送される。そして、制御部 19 の制御によって、受信したコンテンツデータを、表示部 3 の表示画面 3a に表示出力させる。このようにして表示されたメッセージの内容を見ることで、ユーザは、新しい地図情報のディスクがメーカー側から提供されていることを知ることができる。

15 なお、このようなコンテンツデータを受信したときに、ユーザが必ず自動車に搭乗していて表示画面 3a に表示されるコンテンツデータを見ることがあるとは限らない。そこで、例えば運転が行われていないなどして、ナビゲーションシステム 1 のメイン電源が入っていないようなときには、無線端末装置 50 によりコンテンツデータを受信したときに、自動的にメイン電源をオンとして、受信して取得したコンテンツデータをメモリ 12 や記憶部 45 に記憶させておくようになる。そして、例えばユーザが自動車のイグニッションキーを回して、ナビゲーションシステム 1 のメイン電源がオンとなったときに、このコンテンツデータを表示画面 3a に表示させるようにすることも考えられる。

20 もしくは、ナビゲーションシステム 1 が動作している状態のも

バージョンアップが行われることになる。しかも、この場合にはバージョンアップが自動的に行われるため、ユーザにとっては非常に有用なサービスとなるものである。

5 また、携帯電話 200 をユーザが利用して操作を行うことで、遠隔地から自動車についてのセキュリティに関するコントロールを行えるようにすることも可能とされる。この動作についても簡単に説明する。

10 例えは、ユーザは、携帯電話 200 を操作して、無線電話通信網 300 のアプリケーションサーバ 303 に対してアクセスする。ここでアクセスするのは、自動車のセキュリティコントロールのためのサーバ（アプリケーションサーバ 303 に在るものとする）とされる。そして、更にユーザは所定操作を行うことで、自動車の鍵がロックされているか否かについての問い合わせを行う。このリクエストに応じて、アプリケーションサーバ 303 内のセキュリティサーバは、アクセスしてきた携帯電話と同じユーザが所有するナビゲーションシステム 1 のナビ ID を検索して、この検索されたナビ ID のナビゲーションシステム 1 に対して、キーロック問い合わせのコマンドを送信する。

15

20 このコマンドを受信したナビゲーションシステム 1 では、セキュリティシステム部 41 のロックコントロール部 44 からの情報に基づいて、現在鍵がロックされているか否かについてのキーロック情報を、アプリケーションサーバ 303 に送信する。アプリケーションサーバ 303 は、このキーロック情報を、携帯電話 200 に対して転送するようにして送信する。携帯電話 200 では、例えばキーロック情報に基づいて、ユーザの自動車の鍵がかかっているか否かの情報を、例えば表示などによって示すようにされる。

25

そして、例えば鍵がかかっていないとすると、ユーザは、携帯

限定はしないが、ここでは、例えば更新前の地図情報との差分データのみを有しているものとする。つまり、例えば新たな道路を地図上に加えるようにして更新が行われているとすれば、この新たな道路をしかるべき位置に表示させるための差分データが更新データとされることになる。このようにして、更新データを差分データの形式とすれば、例えばサービスサーバ 500 では、サービス用データ 512 に格納すべき更新データとして、更新内容を含む全地図情報を記憶する必要はなくなるので、それだけ、記憶部 801 の記憶容量を節約することができる。

この場合の地図情報が更新されたことのユーザへの通知は、先の地図情報を記録したメディアの最新版の購入を勧めるコンテンツデータの送信と同様にして行えばよいものとされる。そして、送信されたコンテンツデータがナビゲーションシステム 1 にて表示されることで、例えばユーザは、地図情報が更新されており、また、この更新データをダウンロードして取得可能であることを知ることができる。

そして、ユーザが地図情報の更新データを取得したいと思った場合には、例えば、地図情報のダウンロードを指示するための所定操作をナビゲーションシステム 1 に対して行うようにされる。この操作は、例えば上記したコンテンツデータとして含まれている XML や HTML などによるダウンロード用のアプリケーションを GUI として表示画面 3-a に表示させ、この GUI に対して所定操作を行うことができるように構成することが考えられる。

上記のようにして操作が行われたとすると、ナビゲーションシステム 1 においては、例えば制御部 19 の制御によって、自身のナビ ID と共に、更新データのリクエストを送信することになる。この送信データは、通信端末装置 50 から無線電話通信網 300 に対して送信され、無線電話通信網 300 内のアプリケーショ

データが受信されることになる。

そして、ナビゲーションシステム1側においては、受信した更新データを記憶しておくようになされる。以降においては、この更新データを利用することで、地図上の現在位置表示や各種ガイド情報の表示などのナビゲーション動作として、更新データの内容を反映させることができるものである。

また、ユーザにとってメリットのあるサービスではないが、ナビゲーションシステム1の購入後におけるユーザに対する対応として、次のようなことを行うこともできる。

この場合、サービスサーバ500としては、ユーザが分割払いによってナビゲーションシステム1を購入した際には、その支払い状況のデータベースが格納されているものとされる。そして、上記したデータベースの内容から、ユーザの支払いが或る限度以上にまで滞っていることが分かった場合には、サービスサーバ500側から、例えば「代金支払いを御願いします。代金支払いの確認がとれるまで、ナビの利用を停止いたします。」というメッセージと、制御情報を送信する。これを受信したナビゲーションシステム1では、表示画面3aに上記した内容のメッセージを表示させると共に、以降においては、ナビゲーションシステム1自体がその動作を停止させてしまうようにするものである。

また、本実施の形態のナビゲーションシステム1は、先にも述べたように、単体でも購入可能であるが、自動車保険の購入時においてこれと組み合わせて購入することも可能とされ、例えばこのようにして組み合わせて購入した場合には、両者の金額が更に割り引かれたり、また、分割払いの金利手数料が割り引かれるなどのサービスが行われる。そして、このようにして組み合わせによる購入を行った場合に、上述のようにして代金支払いが滞っている場合には、ナビゲーションシステム1の利用の停止と共に、

る。つまり、本実施の形態としては、サーバ側からのアクセスにより、例えば適切とされる機会に、適切な内容のサービスをナビゲーションシステム1に対して積極的に提供することができるものである。

5

3. 処理動作例

10 続いては、上記のようにして例示した各種サービスのうちから選択したいくつかのサービスを実現する際の処理動作について説明していくこととする。

15 先ずは、サービスサーバ500が提供する、ナビゲーションシステム1のバージョンアップのサービスを実現するための処理動作について、図7のフローチャートを参照して説明する。なお、この図においては、サービスサーバ500、アプリケーションサーバ303、及びナビゲーションシステム1の各々において実行される処理が並列的に示される。また、サービスサーバ500としての処理は制御部503が実行し、アプリケーションサーバ303としての処理は、制御部404が実行し、ナビゲーションシステム1としての処理は制御部19が実行する。

20 例えば、メーカ側によりサービスサーバ500に対してナビゲーションシステム1のシステムのバージョンアップをすべきであるとの指示が行われたとすると、サービスサーバ500の制御部503は、ステップS101としての処理により、或る特定のナビゲーションシステム1に対するアクセス要求を行う。この際には、アクセス要求と共に、アクセスすべきナビゲーションシステム1のナビIDを送信する。このナビIDは、例えば、バージョンアップが必要とされるナビゲーションシステム1の機器を所有しているユーザをユーザデータベース501のユーザ情報から検

受信したレスポンスに格納されるバージョンナンバ及びナビ ID を抽出して、これらの情報を、サービスサーバ 500 に対して送信する。

サービスサーバ 500 は、ステップ S103 によりアプリケーションサーバ 303 からのバージョンナンバの通知を受けると、ステップ S103 において、この通知されたバージョンナンバに基づいて、バージョンアップが必要であるか否かについて判別する。例えば通知されたバージョンナンバが今回のアップデータのバージョンナンバ以上であれば、バージョンアップは不要とされて否定結果が得られるが、今回のアップデータのバージョンナンバよりも小さければバージョンアップが必要であるとして肯定結果が得されることになる。

ここで否定結果が得られれば、このナビ ID を有するナビゲーションシステム 1 に対する通信（アクセス）はこれ以上実行しないようにされるが、肯定結果が得られたのであれば、次のステップ S104 の処理によって、バージョンアップメッセージと、アップデータをナビ ID と共にアプリケーションサーバ 303 に対して送信する。これらバージョンアップメッセージとアップデータは、サービスサーバ 500 の記憶部 501 においてサービス用データ 512 として格納してあるものを読み出することで得るようになる。

アプリケーションサーバ 303 においては、ステップ S205 において、バージョンアップメッセージ、アップデータ、ナビ ID を受信する。そして、続くステップ S206 により、受信したナビ ID のナビゲーションシステム 1 に対して、バージョンアップメッセージと、アップデータを送信する。

ナビゲーションシステム 1 においては、バージョンアップメッセージとアップデータを無線端末装置 50 にて受信して、ナビゲ

先ず、図 8 には、自動車の鍵をかけたかどうかについての問い合わせを携帯電話 200 から自動車に対して行うための処理動作が示される。

例えばユーザが携帯電話 200 に対する所定操作を行うことによって、ステップ S 401 として示す、セキュリティリクエストを端末 ID と共に送信するための処理が実行される。このためには、例えば先ず、携帯電話 200 が通信を行ってアプリケーションサーバ 303 内で運営されているとされるセキュリティシステムのサーバにアクセスするようになります。そして、このサーバに対して、自分が所有する自動車についてのセキュリティの問い合わせを要求するものである。この際、自分以外のユーザによる悪用を防止するために、ユーザが予め登録してあるパスワードの入力が求められる。

上記したセキュリティリクエスト、端末 ID、及びパスワードをステップ S 501 により受信したアプリケーションサーバ 303 (セキュリティシステムのサーバ) では、ステップ S 502 の処理として、先ずユーザデータベース 410 を参照して、パスワードと端末 ID などとの照合を行うことで認証処理を実行する。つまり、セキュリティリクエスト、端末 ID、及びパスワードを送信したユーザが正規のユーザであることについての確認を行う。なお、この時点で認証が得られなければ、以降の処理は停止される。

そして適正に認証が得られたとされると、次のステップ S 503 において、そのユーザデータベース 410 において、認証された端末 ID 及びパスワードに対応付けられたナビ ID を検索して得る。そして、続くステップ S 504 により、取得したナビ ID (電話番号) を有するナビゲーションシステム 1 に対してセキュリティリクエストを送信する。

携帯電話 200 では、この送信されたセキュリティチェックの結果データが着信したことをステップ S402 にて判別すると、これを受信して、次のステップ S403 において、例えば ROM 217 に対して記憶させるようにしている。そして、例えばこの後において、ユーザが所定操作を行うことで、ステップ S404 としての処理によって、このセキュリティチェックの結果を文字等により LCD 表示部 209 に表示させることができるようになっている。

そして、例えば LCD 表示部 209 に表示させたセキュリティチェックの結果から、自動車に鍵がかかっていないことをユーザが知った場合には、前述したようにして、携帯電話 200 からのリモートコントロールによって、自動車の鍵をかけることが可能とされている。このための処理が図 9 に示される。

ここでは、例えばユーザの所定操作に応じて、ステップ S701 の処理によって、携帯電話 200 のインターネット接続機能を利用してアプリケーションサーバ 303 に対してアクセスする。そして、自動車の鍵をかけることを指示するためのキーロック指示情報を、携帯 ID とパスワードと共に送信する。

アプリケーションサーバ 303 では、ステップ S801 としての処理によって、上記キーロック指示情報、携帯 ID、及びパスワードを受信すると、先ず、ステップ S802 の処理によって認証処理を実行する。この認証処理は、図 8 のステップ S502 における認証処理と同様となる。そして、適正な認証結果が得られたのであれば、ステップ S803 に進む。

ステップ S803 においては、ユーザデータベース 410 を参照することで、携帯 ID と対応付けられたナビ ID を検索する。そして、次のステップ S804 において、検索したナビ ID を有するナビゲーションシステム 1 に対してキーロックコマンドを送

5 をステップ S 2 1 により受信したアプリケーションサーバ 3 0 3 では、次のステップ S 2 2 の処理として、ユーザデータベース 4 1 0 を参照して、登録されているパスワードとナビ I D などとの照合を行うことで認証処理を実行する。つまり、更新データのリクエストを送信したユーザが正規のユーザであるか否かについての確認を行う。なお、この場合にも、認証が得られなければ以降の処理は停止される。

10 そして適正に認証が得られたとされると、次のステップ S 2 3 において、先のステップ S 2 1 にて受信したとされるリクエスト

15 とナビ I D を、サービスサーバ 5 0 0 に対して送信する。サービスサーバ 5 0 0 では、ステップ S 3 1 の処理として、アプリケーションサーバ 3 0 3 から送信されたリクエストとナビ I D を受信すると、次のステップ S 3 2 において、記憶部 5 0 1 にてサービス用データ 5 1 2 として記憶されている、地図情報の更新データのファイルについての読み出しを行う。

20 なお、この更新データは、例えば前述もしたように、更新前の地図情報としてのデータに対する差分データとされればよい。また、ここでは、全ての更新データファイルについて読み出しを行ってもよいが、例えば、この更新データが商品として購入されるものであって、例えばユーザが指定した地域数等に応じてその価格が代わるように設定することも考えられる。そこで、このような場合であれば、リクエストとしては、ダウンロードすべき更新データファイルを指定する情報を含むようにして、この指定された更新データファイルのみについての読み出しを行うようにしてもよい。

25 上記のようにして更新データファイルの読み出しが行われると、続いては、ステップ S 3 3 の処理によって、読み出した更新データファイルを、先にステップ S 3 1 においてリクエストと共に

映されたナビゲーション動作が得られることになる。

また、記録媒体9が書き換え不可である場合には、例えば電源がオフとなっても記憶内容が維持されるメモリ12若しくは記憶部45などに受信した更新データを記憶させておく。そして、地図情報を利用した表示を行うような場合には、例えばメモリ12若しくは記憶部45に記憶されている更新データを読み出して、記録媒体9から読み出した地図情報に合成させて、更新データが反映された地図情報を形成する。そして、この地図情報を利用してナビゲーション動作を行うようにされる。

なお、先にも述べたように、このような更新データの提供サービスは、有料とすることも無料とすることも考えられるが、有料であるとすれば、ナビゲーションシステム1から送信されたダウンロードのリクエストをサーバ側で受信したときに、例えばユーザが指定した支払方法に応じた決済の処理が行われるようにすればよい。

4. サービス提供システム（第2例）

4-1. 全体構成

続いては、実施の形態の第2例としてのサービス提供システムについて説明していくこととする。

図11は、第2例としてのサービス提供システムの一形態例を示している。

この図に示されるように、第2例としては、図1に示した第1例のシステム構成に対して、装置としては、パーソナルコンピュータ700と、認証サーバ800が追加された構成を探っている。そこで、図11の説明にあたっては、これらの追加部分等の相

例えばほかには、I S D N (Integrated Services Digital Network)、また、電話回線の高周波帯域を通信に利用したA D S L (Asymmetric Digital Subscriber Line)等をはじめとするx D S L、C A T V、無線通信網などを挙げることができる。

5 認証サーバ800は、例えば後述するようにして、パーソナルコンピュータ700が自動車100の現在位置情報を得るために、自動車100に搭載されているナビゲーションシステム1に対してアクセスする際に、このアクセスが適正なものであるか否かについて認証を行うために設けられている。この認証サーバ800が機能することによって、結果的には、例えばいわゆる成りすましによって、正規に登録されていないパーソナルコンピュータが自動車100から現在位置情報を得るという不正行為を防止するようにされる。

10 15 なお、認証サーバ800の内部構成及びその動作については、後述する。

4-2. パーソナルコンピュータの内部構成

20 図12は、パーソナルコンピュータ700の内部構成例を示している。

この図に示すパーソナルコンピュータ700は、インターネット400を介しての通信を行うために、ネットワークインターフェイス709を備えている。ネットワークインターフェイス709は、アクセス用通信網600と当該パーソナルコンピュータ700との通信を司るのであるが、これによって、パーソナルコンピュータ700は、アクセス用通信網600を介してインターネット400と接続されることになる。

C P U 701は、例えばハードディスクドライブにインストー

照して説明する。

この図に示す認証サーバ 800 は、記憶部 801、ネットワークインターフェイス 802、制御部 803 を備える。

5 認証サーバ 800 の場合、記憶部 801 には、後述する認証処理等を実行するのに必要とされる情報が記憶されている。ここでは、記憶部 801 に格納されるデータとして、認証用ユーザデータベース 810、実行アプリケーション 811 が示される。

10 認証用ユーザデータベース 810 は、例えば図の下側に示すように、1 ユーザごとに、ユーザ情報、携帯 ID、ナビ ID、PC-ID、コンテンツ ID、及び PC 用パスワードが対応づけられて格納される。

15 ユーザ情報は、ナビゲーションシステム 1、携帯電話 200、及びパーソナルコンピュータ 700 を組として所有するユーザに関する情報であり、例えば本実施の形態のシステムの場合であれば、サービスサーバ 500（又はアプリケーションサーバ 303）に格納されるユーザデータベース 510（410）を形成するユーザ情報と同じ内容とされればよい。

20 携帯 ID は、ユーザ ID によって特定されるユーザが所有する携帯電話に書き込まれている携帯 ID と同一のデータが格納される。ナビ ID も同様にして、ユーザが所有するナビゲーションシステム 1 に割与えられたものと同一のナビ ID のデータが格納される。また、このナビ ID として、無線端末装置 50 に対して割り与えた電話番号とされればよい。つまり、この場合の携帯 ID 及びナビ ID は、図 5 にて説明したユーザデータベース構造において格納される情報と同じ情報が格納されればよいものである。

25 PC-ID は、ユーザ ID によって特定されるユーザが所有するとされるパーソナルコンピュータ 700 を識別するための ID とされる。本実施の形態としては、この PC-ID の構造に特徴

5

10

15

20

25

るユーザが、現在、自己の所有しているナビゲーションシステム1を搭載している自動車100の現在位置を知りたいと思ったとする。この場合、ユーザは、パソコンコンピュータ700上で、例えばWebブラウザのアプリケーションを起動させた上で、所定操作を行って、現在位置通知サービスのWebサイトにアクセスするようになる。この現在位置通知サービスのWebサイトは認証サーバ800にてアップロードしているWebサイトとされる。つまり、ユーザが現在位置通知サービスのWebサイトにアクセスしたことによって、パソコンコンピュータ700は、認証サーバ800にアクセスしたこととなる。

上記のようにして認証サーバ800に対してアクセスしたすると、ユーザは、現在位置情報通知のためのリクエストを送信するようになる。また、この現在位置情報通知のリクエストとともに、認証サーバ800が認証で用いるべき所要の認証情報も送信するようになる。

なお、認証情報がどのようなものであるのかについては後述する。

また、認証サーバが認証に用いる認証情報としては、リクエストを送信したパソコンコンピュータ700に固有となるPC-IDを含むが、このPC-IDは、パソコンコンピュータ700にて生成して送信されるのではなく、パソコンコンピュータ700が接続されるアクセス用通信網600内において、例えばアプリケーションサーバとして機能する部位が、パソコンコンピュータ700が認証サーバ800にアクセスしてきたときに生成するようになる。このPC-IDの生成及びユーザデータベース810への登録についても後述することとする。

認証サーバ800では、上記のようにして、現在位置情報通知のリクエストと共に送信されてきた認証用情報と、ユーザデータ

に、ユーザがパーソナルコンピュータ 700 を認証サーバ 800 にアクセスさせ、所定の登録のための操作を行うことで登録が行われるようにすることが考えられる。

つまり、ユーザはパーソナルコンピュータ 700 を操作して、
5 例えは認証サーバ 800 における登録用の Web ページにアクセスする。この Web ページには図 13 に示した認証用ユーザデータベース 810 を構築するのに必要とされる、1 ユーザについての所要の情報項目を入力することができるようになっている。つまり、「ユーザ情報」となる氏名、住所等をはじめとする個人情報、ユーザが所有する携帯電話 200 の「携帯 ID (電話番号)」、同じくユーザが所有するナビゲーションシステム 1 の「ナビ ID (電話番号)」、及び「サービス ID」に対応する享受したいサービス内容 (この場合には、現在位置通知サービスとなる) を入力するようになれる。例えば認証サーバ 800 においては、現在位置通知サービス以外のサービスも対応して認証を行うような構成とすることも充分に考えられるが、サービス ID は、このような場合において、ユーザがサービスの提供を要求してきたときに、そのサービスが何であるのかを識別するのに用いることができる。

20 また、例えは本実施の形態としての現在位置通知サービスに關すれば、携帯電話 200 はこのサービスを享受するのに利用はしていないので、必ずしも、携帯 ID を認証用ユーザデータベース 810 の情報要素とする必要はない。しかし、やはり、認証サーバ 800 において現在位置通知サービス以外のサービスも対応して認証を行うこととして、その他のサービスが携帯電話 200 を利用するものであるような場合には、携帯 ID が必要となるものである。

また、図 13 によれば、上記「ユーザ情報」「携帯 ID (電話

5

テム構成に加えたとすると、このパーソナルコンピュータ 700 は、無線電話通信網 300 にアクセスすることなく、例えば電話回線等をはじめとする何らかのアクセス用通信網 600 を介してインターネットにアクセスすることになる。このような場合には、前述した成りすましの問題が生じてくるわけであり、この問題を解決する必要が生じてくるものである。

10

そこで本実施の形態としては、次のようにして PC-ID を生成して認証サーバに登録することで、機器 ID を改竄しての成りすましによる不正なサービスの享受ができないようにする。なお、ここではアクセス用通信網 600 として実際に利用される通信網の種類に応じて、3 例を挙げることとする。

15

図 14 は、PC-ID 登録手順の第 1 例を模式的に示している。この第 1 例は、アクセス用通信網 600 が一般電話回線、若しくは ISDN 回線とされている場合である。

20

25

アクセス用通信網 600 が一般電話回線、若しくは ISDN 回線などの場合、パーソナルコンピュータ 700 がインターネットと接続されるためには、いわゆるダイヤルアップを行うことになる。つまりは、ここでは図示していないが、パーソナルコンピュータ 700 側が備えるとされるモデム、TA (Terminal Adapter)、DSU (Digital Service Unit) から、アクセス用通信網 600 において一般電話回線又は ISDN 網として実際に配置される設備である電話局 601 に対してダイヤリングをして接続する。

ここで、留意すべきなのは、上記電話局 601 に対してダイヤルアップを行うということは、このダイヤルアップを行うために割り当てられた電話回線、ISDN 回線についての電話番号が一義的に決まっているということである。この電話番号は、電話局 601 にて管理している以上、パーソナルコンピュータ 700 のユーザによっては改竄することのできない情報であるといえる。

601側にて管理するものであり、かつ、PC-IDは電話局601側にて作成するものであるから、パーソナルコンピュータのユーザが、この電話番号部分を書き換えることは不可能である。従って、パーソナルコンピュータについていわゆる成りすましを行ふことは不可能となるわけである。

5 そして、電話局601からは、このようにして生成したPC-IDをインターネットを介して認証サーバ800に送信することになる。

10 このPC-IDを受信した認証サーバ800では、手順③として示すように、受信したPC-IDを、他の情報（ユーザ情報、携帯ID、ナビID、及びサービスID）と共に、認証用ユーザデータベース810に登録するようになれる。

15 また、PC-ID登録手順の第2例を図1.5に示す。この第2例は、アクセス用通信網600がADSLなどの常時接続が可能な通信網とされている場合である。

20 このような通信網である場合、例えばアクセス用通信網600における設備である電話局601においては、例えば電話回線を、一般電話回線とインターネットの経路とに分岐するスプリッタなどのポート部が設けられることになるのであるが、この図においては、このようなポート部を接続ポート602, 602...として示している。

25 例えば、電話局601では、加入者がADSLに加入したときに接続ポート602の工事を行って加入者の電話回線と接続するようにしている。従って、この接続ポート602については、電話局601側が管理するものであると共に、接続される電話回線も固定的なものとなっているといえる。

そこで、本実施の形態としては、例えば電話局601において接続ポート602ごとに識別子（ポートID）を割与えて管理す

ソナルコンピュータ 700 が常時接続される。

5 このような場合、パーソナルコンピュータ 700 は、専用線 610 において備えられるとされるルータ 611 に対して接続され、このルータ 611 からインターネット 400 への接続が行われる。そして、この場合には、パーソナルコンピュータ 700 は、ルータ 611 に対して常時接続されているのであるから、パーソナルコンピュータ 700 とルータ 611 との経路は固定されていることになる。また、このルータ 611 の管理も専用線 610 側の運営者によって行われていることになり、このルータ 611 に関する情報をパーソナルコンピュータ 700 側のユーザが改竄することはできないとされる。

10 そこで、第 3 例としては、パーソナルコンピュータ 700 の機器 I D と、ルータ 611 に固有となる情報を利用して PC - I D を形成するようにされる。そして、この場合には、ルータ 611 に固有となる情報としては、ルータ 611 に割り当てられたルータアドレスを使用することとする。

15 そして、この第 3 例としての PC - I D 登録手順は以下のようになる。

20 先ず、手順①として、パーソナルコンピュータ 700 からは、認証サーバ 800 に向けて機器 I D を送信する。この場合においても、機器 I D の送信は、実際には、「ユーザ情報」「携帯 I D (電話番号)」「ナビ I D (電話番号)」、及び「サービス I D」の各情報とともに送信するものとされる。

25 但し、この場合の機器 I D としては、先の第 1 例及び第 2 例の場合のようにして、メーカコード-製造番号から成る情報を使用してもよいのであるが、常時接続されていることを前提とすると、例えば DHCP (Dynamic Host Configuration Protocol) によるものであるとしても、最初に I P アドレスの割り当てが行われ

これまでの説明からも理解されるように、アクセス用通信網 600 と接続するまでの通信経路は、パーソナルコンピュータ 700 が例えば屋内等において固定的に設置されるということを前提にすれば、そのパーソナルコンピュータ 700 と通信経路とは 1 対 1 で固定的に対応するものとなる。従って、上記通信経路を特定する情報と機器 ID とを組み合わせたとしても、パーソナルコンピュータ 700 に固有となる PC-ID を形成するのに何ら問題はないことになる。また、先の説明でも述べたようにして、通信経路を特定する各情報（電話番号、接続ポートのポート ID、ルータアドレス）は、何れもアクセス用通信網 600 を運営する設備側で管理しているものであり、悪意のパーソナルコンピュータ 700 のユーザがこれを改竄することはできないとされる。従って、この情報をを利用して生成される PC-ID をパーソナルコンピュータ 700 のユーザが改竄することもできないわけである。また、本実施の形態としては、PC-ID は、パーソナルコンピュータ側ではなく、中継点であるアクセス用通信網 600 の設備側で生成するようにされていることによっても、改竄される可能性を著しく低いものとしている。

つまり、本実施の形態の PC-ID としては、パーソナルコンピュータを特定可能としながら、かつ、改竄による成りすましを防止することのできる情報となっているものである。これによって、先にも述べたように、成りすましによるパーソナルコンピュータ 700 を利用してのサービスの提供が行われるのを防止することが可能となる。

なお、本発明としては、パーソナルコンピュータ 700 が最初に接続される通信網（アクセス経路）を特定できる情報でありさえすればよく、上記図 14～図 16 により例示した登録手順における PC-ID の生成例以外にも、本発明に適合する PC-ID

際には、ユーザ情報、機器ID、及びサービスIDと共に送信するようにされる。

例えば現在位置通知サービスのブラウザ画面上には、リクエストに必要とされる各種項目を入力する入力ボックスが表示されるようになっているものとされる。上記ユーザ情報は、この入力ボックスに入力した例えば住所、氏名等の個人情報に基づいて、ユーザを特定するIDとしてCPU701が作成する。

また、機器IDは、例えばこれがメーカコードと製造番号から成るものであるとすれば、CPU701が例えばROM702から読み出したメーカコード、製造番号の情報に基づいて作成することになる。また、機器IDがIPアドレスであれば、例えばRAM703に保持しているIPアドレスを利用して作成する。

また、サービスIDは、例えば、このリクエストが現在位置通知サービスに対応したものであることを示すIDとして、現在位置通知リクエストとしてのデータ構造内に格納されているものとする。

上記のようにして送信された現在位置通知リクエストは、図14～図16にて説明したようにして、まずは、アクセス用通信網600にてルーティングされ、インターネット400を介して認証サーバ800に転送されることになる。そして、この際ににおいて、アクセス用通信網600の設備においては、受信取得した機器IDと、自身が管理して保有しているとされる経路特定情報（電話番号、ポートID、ルータアドレスなど）を利用してPC-IDを作成する。従って、認証サーバ800に対しては、現在位置通知リクエストと共に、このPC-IDと、ユーザ情報、サービスIDが送信されることになる。

認証サーバ800では、上記のようにして送信されてきた現在位置通知リクエスト、ユーザ情報、PC-ID、及びサービスI

は、ステップ S 6 1 の処理によって現在位置通知リクエストを受信することになる。

ここで、本実施の形態のナビゲーションシステム 1 は現在位置通知サービスに対応したプログラムを格納している。このプログラムは、受信した情報が現在位置通知リクエストである場合には、測位部 4 にて測定される現在位置情報と、例えば記録媒体 9 等から読み出した地図情報とを利用して現在位置情報を作成し、認証サーバ 800 にアクセスして送信を行うという動作を実行させるものである。なお、現在位置情報の生成に利用する地図情報としては、例えば前述したようにして取得した更新データがあれば、この更新データも利用するようにされる。そして、次に述べるステップ S 6 2 ～ S 6 4 の処理は、このプログラムに従って実行される。

ステップ S 6 2 においては、現在位置情報を作成する。

前述もしたように、ここで作成される現在位置情報は、例えば Web ブラウザによって表示可能な HTML や XML などの形式とされ、Web ブラウザ上で再生すれば、地図上に現在位置が示される画像を表示させることができるデータ内容を有しているものとされる。なお、例えば JPEG、JIF、及びビットマップなどをはじめ、単に所定の形式による画像データとして生成することも考えられる。

そして、次のステップ S 6 3 においては、ナビゲーションシステム 1 が認証サーバ 800 に対してアクセスするための制御処理を実行する。このため、例えばナビゲーションシステム 1 においては、例えばメモリ 12 などに認証サーバ 800 の URL が保持されているものとされ、制御部 19 は、この URL にアクセスが行われるように、通信インターフェイス 47 から通信端末装置 50 を介してアクセス要求を送信させる。

5

また、認証サーバ 800 としては、例えば当然のことではあるが、1つの装置としてではなく、例えば処理負担の軽減のために、認証サーバ 800 として機能する複数の装置が、インターネット上において分散するようにして設けられた構成としても構わないものである。

また、不正行為を防止する構成としては、次のような構成を補助的に付加することも考えられる。

10

15

20

25

例えば本実施の形態としてのサービス提供システムにおいて、ユーザがサービス提供に利用するものとして登録している各機器（ナビゲーションシステム、携帯電話、パーソナルコンピュータ等）のインターネットの接続を、特定の1つの通信会社（電話会社等）が行うとする。そして、例えばこの通信会社がカバーする範囲の通信網内において監視サーバを設けるようとする。監視サーバは、ユーザが登録している各機器間の通信として、この通信会社がカバーする一定範囲内の回線を利用しているか否かを監視するようとする。そして、通信会社がカバーする一定範囲外の回線から入ってくるようにして、ユーザが登録している機器が通信を行う状況となった場合には、何らかの警告を与えたり、また、不正のサービス利用が行われるような回線の利用状況であるとする場合には、通信を中断させるようにするものである。

また、本発明としては上記した各実施の形態に限定されるものではない。例えば、提供すべきサービスとしては、これまで例示したもの以外にも各種考えられる。また、サービス提供に利用される機器としては、カーナビゲーション装置、携帯電話、パーソナルコンピュータ等に限定されるものではなく、例えばインターネットなどのネットワークとの接続機能を有する移動通信端末装置を備える機器や、また、移動通信端末装置ではなくとも、特定の通信網を介してインターネットと接続される通信端末装置を備

ムを購入したユーザにとっては、サービス提供をこれまでよりも簡易で有効なかたちで享受することができ、また、販売側の両者にとっては製品の付加価値が高まるので、販売促進の効果も期待できることになる。

5 また、屋内等に固定的に設置される通信端末装置（パソコン
コンピュータ）から電子機器（例えばナビゲーションシステム）
に対して通信を行う場合においては、認証サーバを介在させるよ
うにしている。また、通信端末装置が電子機器と通信するために
10 認証サーバにアクセスしたときには、アクセス経路を特定する情
報（電話番号、ポート番号、ルータアドレス等）を利用して端末
ID（P C – I D）を生成するようにしている。そして、認証サ
ーバでは、端末IDを利用して認証処理を行うようにしている。

15 アクセス経路を特定する情報は、通常は、通信端末装置が最初
に接続する通信網を運営する側が管理保持していることから、通信
端末装置側にて改竄することは不可能な情報であり、従って、
端末IDとしても改竄することのできない情報であるといえる。
つまり、この発明によっては、いわゆる成りすましによって不正
なサービス利用が行われることを、簡易な構成によって確実に防
止することができるものである。

20

産業上の利用の可能性

この発明は、例えば自動車などの移動体に搭載される電子機器
と、サーバ及び携帯電話などの個人移動端末装置とを通信網を介
して通信可能なように構築されたシステムとして、例えば電子機
器を購入して利用しているユーザに対して、送信されたデータを
25 受信した電子機器が、その受信データの内容に従って何らかの動
作の実行を行うことで享受できるようなサービスを提供するこ
のできるシステムに利用される。

有となる端末 I D が割り与えられる移動無線端末装置と、通信網とを備えて成り、

上記移動無線端末装置から上記電子機器に対して、上記機器 I D を利用して上記通信網を介してアクセスし、特定のサービス提供を実現するための所定内容を有するサービス情報を送信するための送信手段、

を備えていることを特徴とするサービス提供システム。

4. 少なくとも、無線通信端末機能を備えて移動体に搭載されると共に、固有となる機器 I D が割り与えられる電子機器と、固有となる端末 I D が割り与えられる移動無線端末装置と、通信網とを備えて成り、

上記電子機器から上記移動無線端末装置に対して、上記端末 I D を利用して上記通信網を介してアクセスし、特定のサービスに利用可能な所定内容の情報を送信することのできる第 1 の通信手段と、

上記移動無線端末装置から特定の電子機器に対して、上記機器 I D を利用して上記通信網を介してアクセスし、アクセスした電子機器に対して、特定のサービス提供を実現するための所定内容を有するサービス情報を送信するための第 2 の通信手段と、

を備えていることを特徴とするサービス提供システム。

5. 少なくとも、無線通信端末機能を備えて移動体に搭載される電子機器又は移動無線端末装置としての電子機器と、通信網と、該通信網にアクセスする経路が固定的となるようにして設置される通信端末装置と、上記通信網に接続される認証サーバとから成り、

上記通信端末装置が、上記電子機器に固有となるように割り与えられる機器 I D を利用して上記通信網を介して上記電子機

報とに基づいて判断して上記無線通信装置を制御する認証装置とを備える通信システム。

7. 上記通信システムは、

5 通信機能を備えるとともに機器毎に異なる第2の機器IDを備える第2の電子装置と、

10 上記第2の電子装置と通信を行うと共に上記ネットワークに接続され、上記第2の機器IDを上記第2の電子装置から受信し、上記第2の電子装置と通信を行う通信手段を特定する通信手段IDと上記第2の機器IDとを上記認証装置に送信する通信装置

を更に備える第6記載の通信システム。

8. 上記認証装置の備えるグループ情報は、上記第2の電子装置を上記第2の機器IDと上記通信手段IDとを関連づけて更に管理する第7項記載の通信システム。

15 9. ネットワークに接続され各々の機器を識別可能とするための機器IDを各々備えるとともに送信可能な複数の他の電子機器の間の通信を制御する通信装置において、

上記ネットワークを通して他の装置と通信を行うための通信手段と、

20 電子機器間の通信が認証されることによって許可される複数の機器がグループ化されて登録されるグループ情報が記憶される記憶手段と、

25 上記複数の電子機器の通信開始前に上記ネットワークを通して送信する機器IDと上記記憶手段に記憶されたグループ情報とに基づいて、電子機器間の通信が許可されているか否かを判別する判別手段と、

上記ネットワーク接続され送られる機器IDに基づいて電子機器を特定して通信を交換処理する交換装置へ、上記判別結果

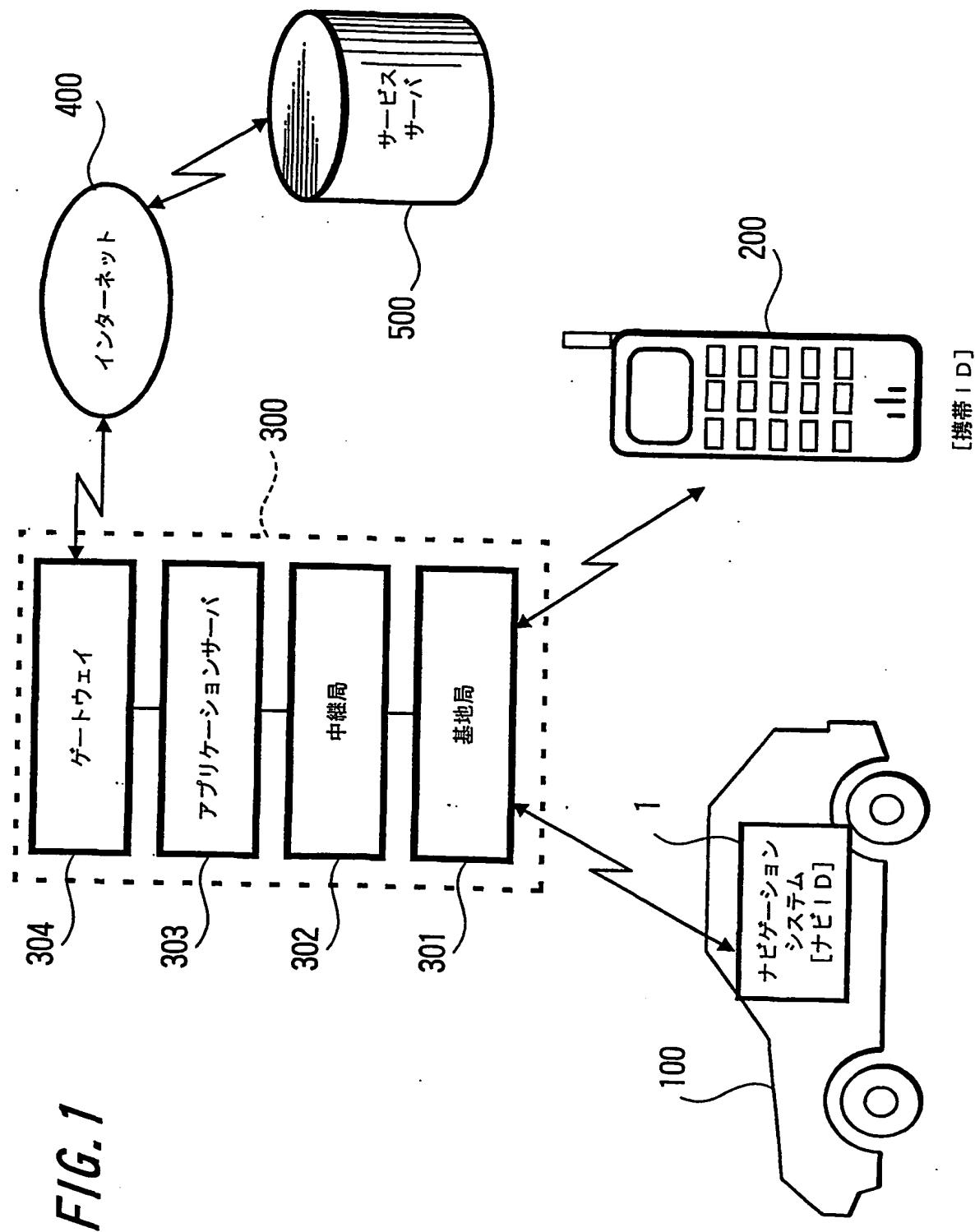


FIG. 1

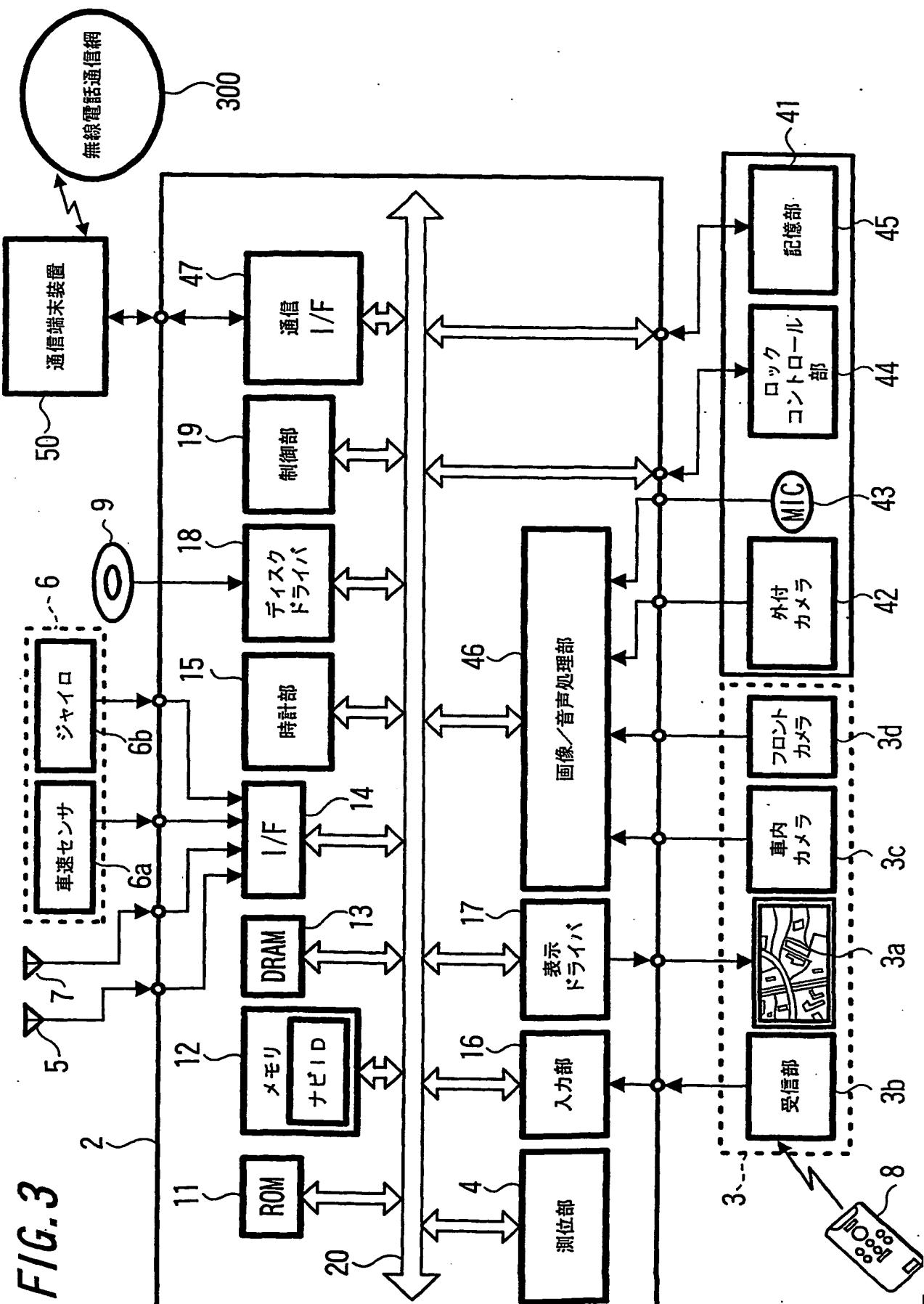


FIG. 5

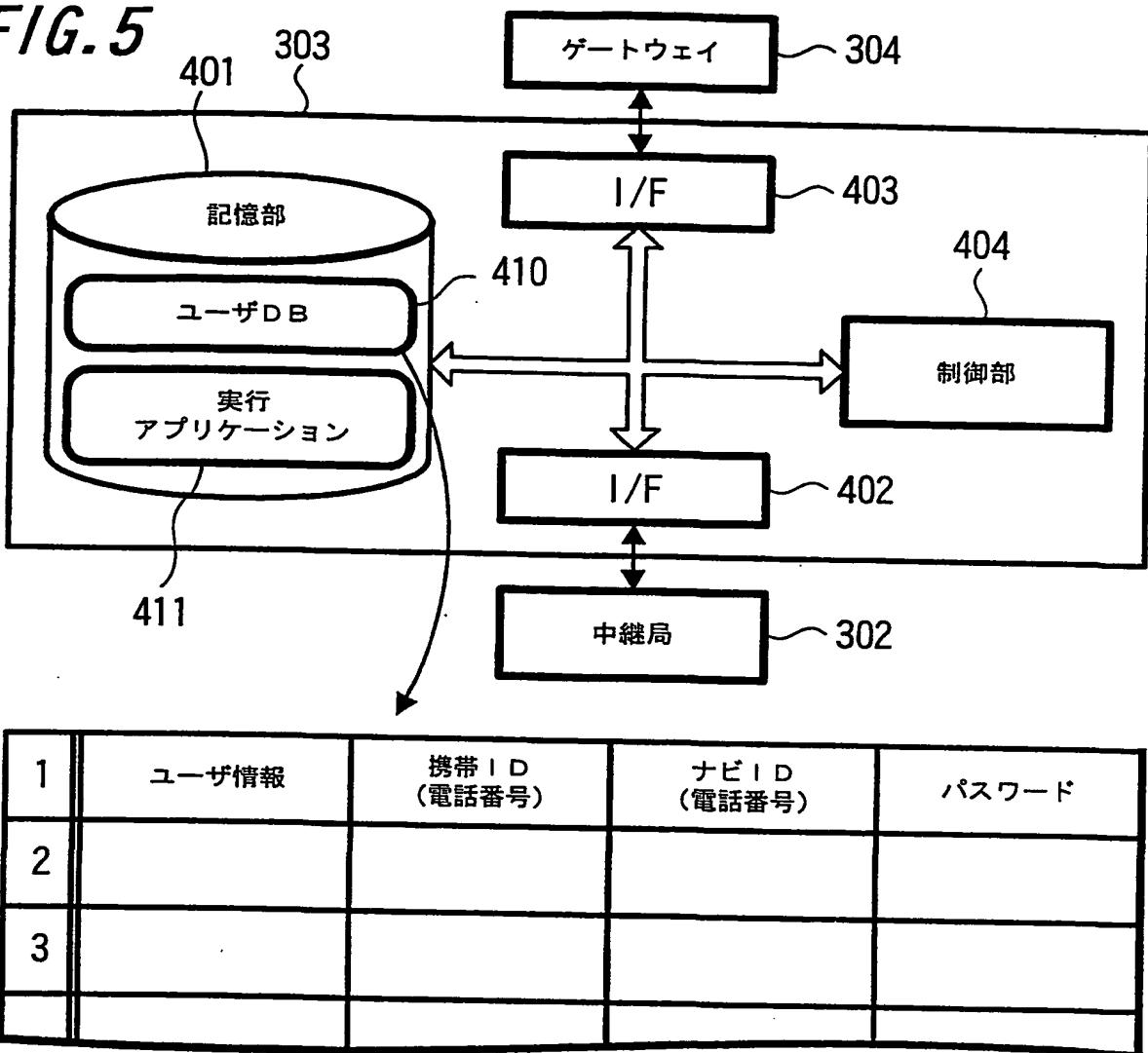
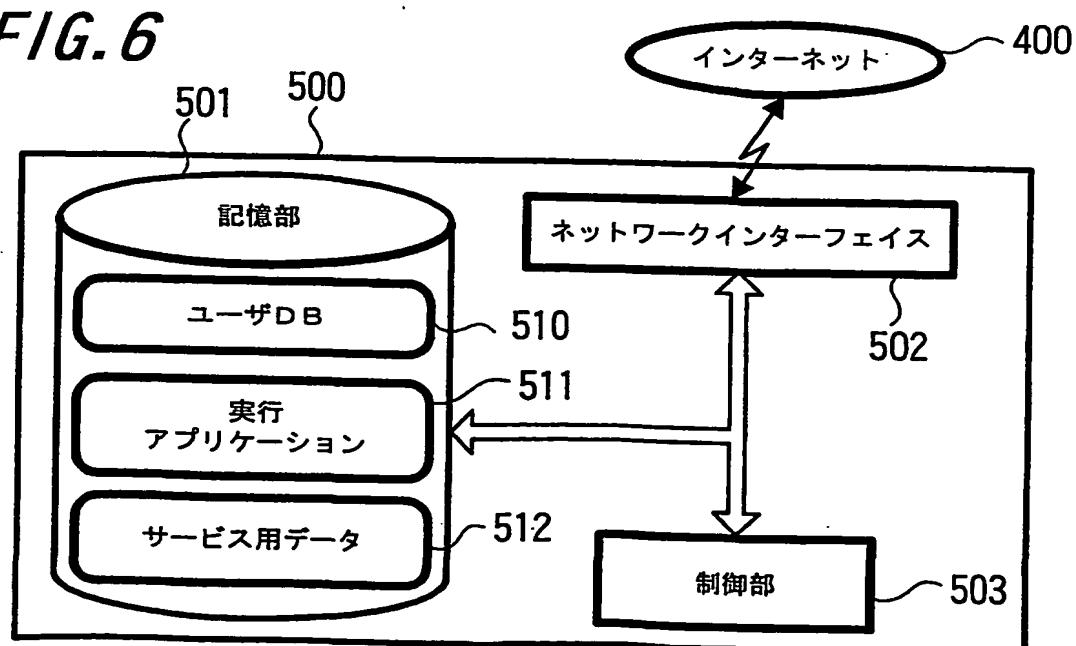


FIG. 6



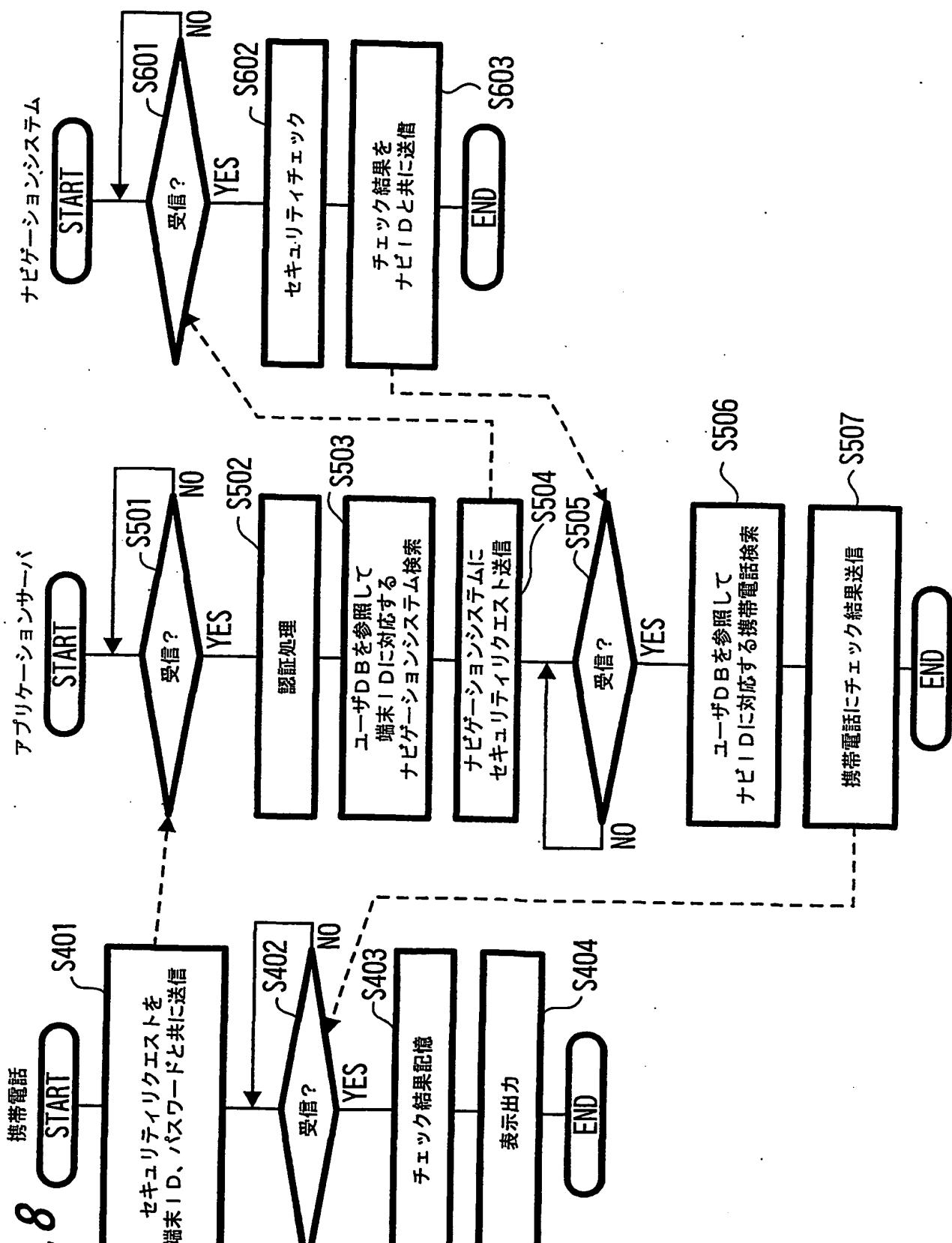


FIG. 10

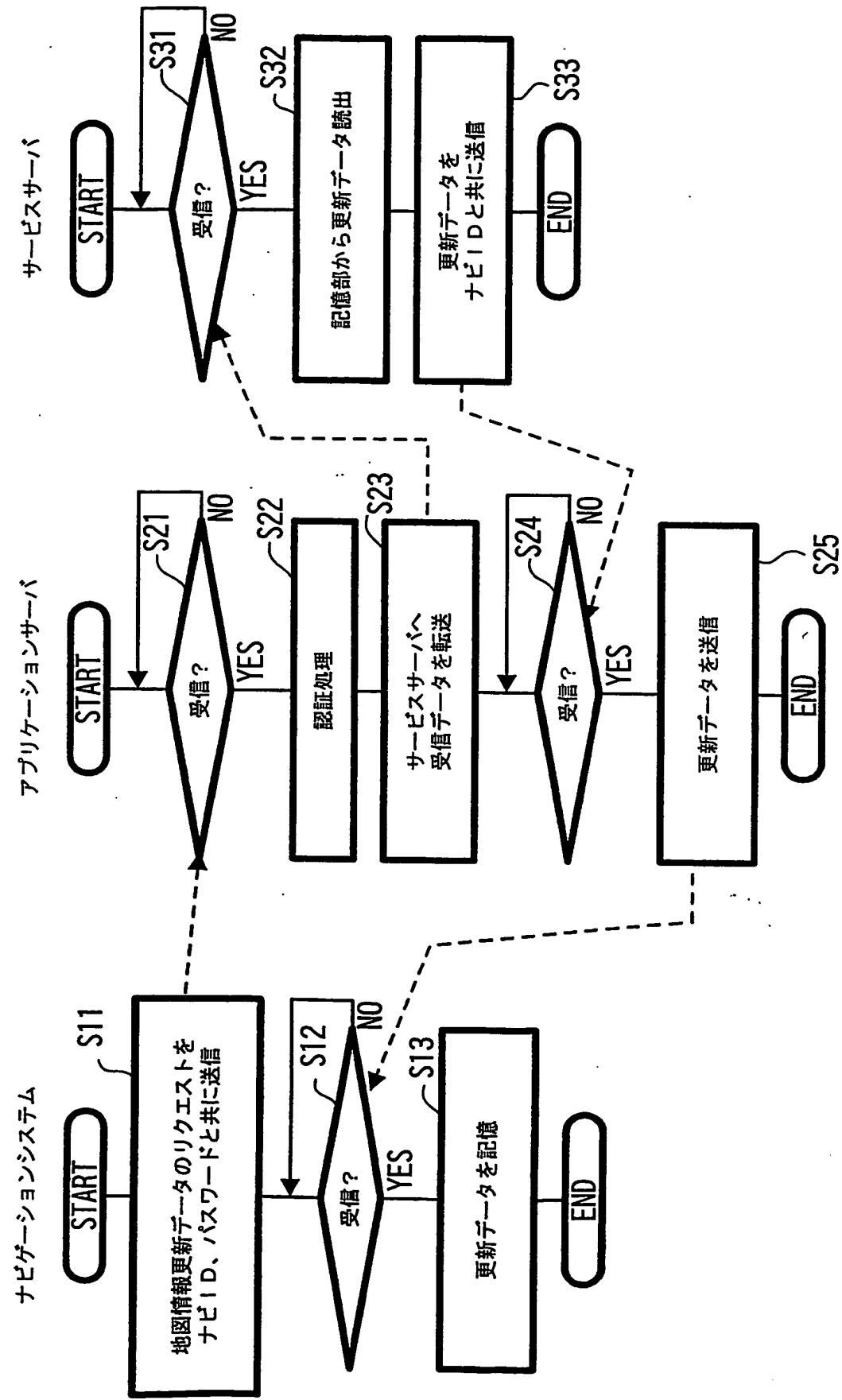


FIG. 12

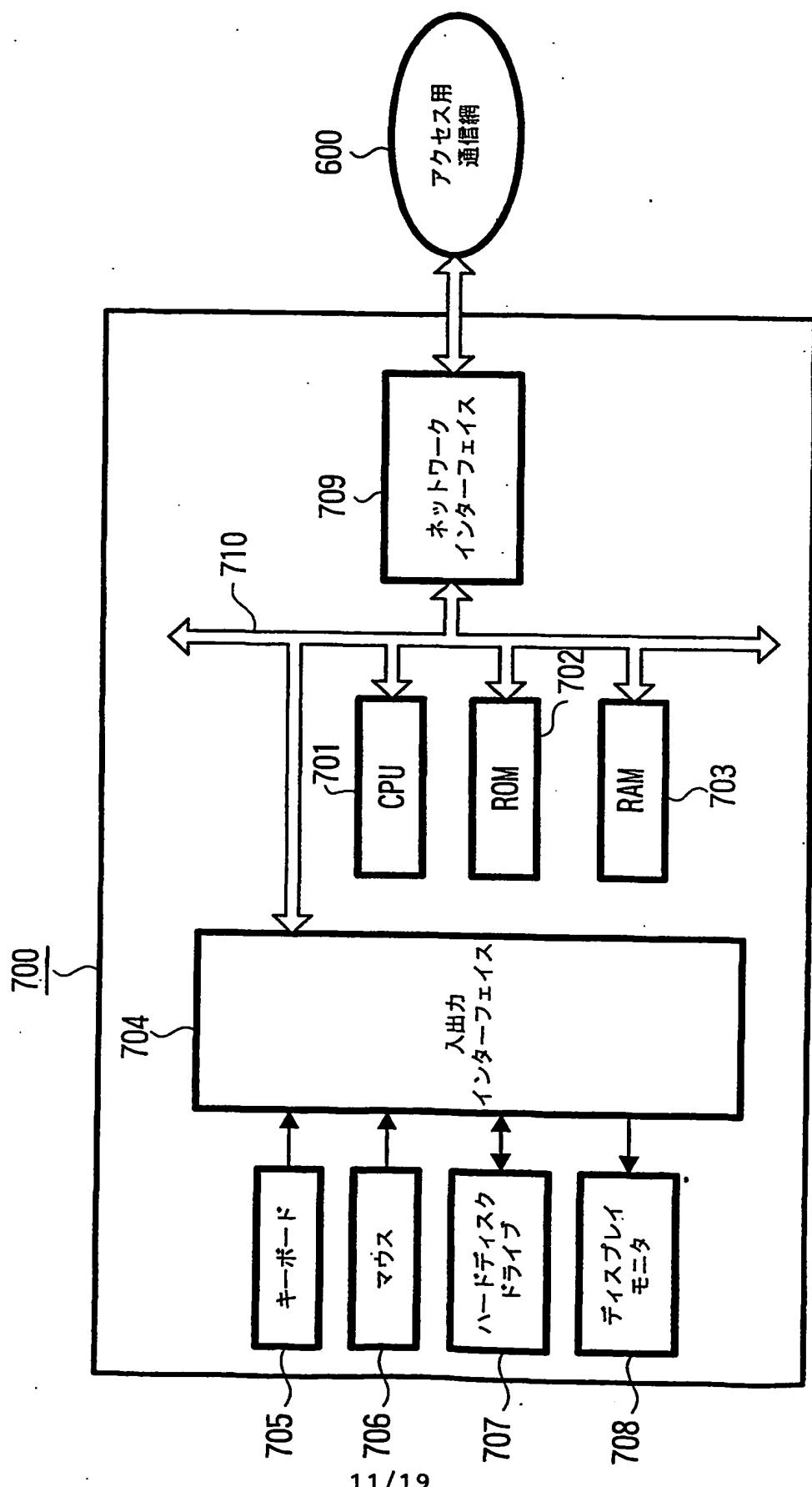


FIG. 14

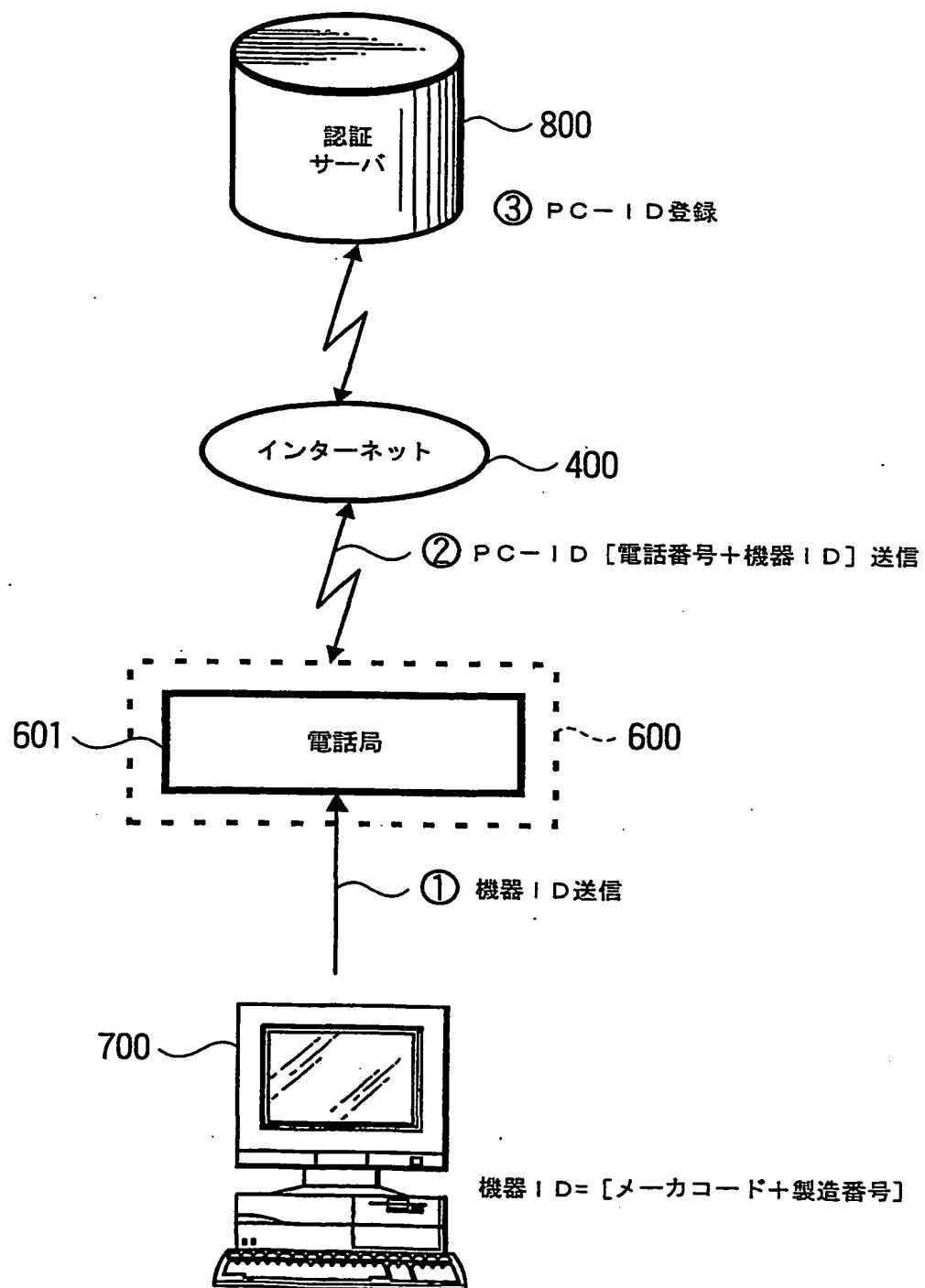
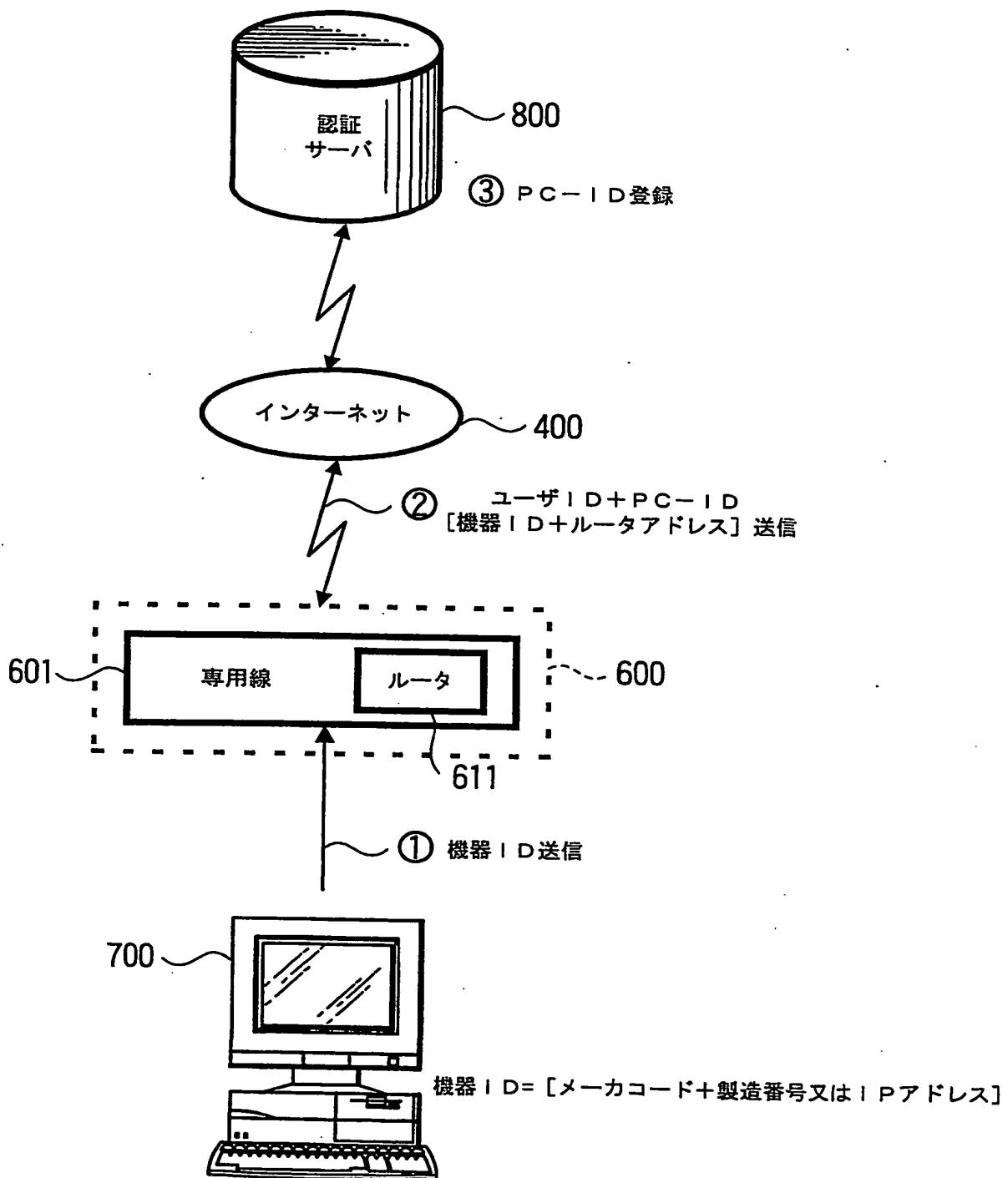


FIG. 16



符 号 の 説 明

- 1 ナビゲーションシステム、
- 2 ナビゲーション本体部、
- 3 ディスプレイモニタ部、
 - 3 a 表示画面、
 - 3 b 受信部、
 - 3 c 車内カメラ、
 - 3 d フロントカメラ、
- 4 測位部、
- 8 リモートコントローラ、
 - 8 a 緊急キー、
- 9 記録媒体、
 - 1 1 R O M、
 - 1 2 メモリ、
 - 1 3 D R A M、
 - 1 4 インターフェイス、
 - 1 5 時計部、
 - 1 6 入力部、
 - 1 7 表示ドライバ、
 - 1 8 ディスクドライバ、
 - 1 9 制御部、
 - 2 0 バス、
- 4 1 セキュリティシステム部、
- 4 5 記憶部、
- 4 6 画像音声処理部、
- 4 7 通信インターフェイス、
- 5 0 通信端末装置、
- 2 0 0 携帯電話、

- 6 0 0 アクセス用通信網、
- 7 0 0 パーソナルコンピュータ、
- 7 0 1 C P U、
- 7 0 2 R O M、
- 7 0 3 R A M、
- 7 0 4 入出力インターフェイス、
- 7 0 5 キーボード、
- 7 0 6 マウス、
- 7 0 7 ハードディスクドライブ、
- 7 0 8 ディスプレイモニタ、
- 7 0 9 ネットワークインターフェイス、
- 7 1 0 内部バス、
- 8 0 0 認証サーバ、
- 8 0 1 記憶部、
- 8 0 2 ネットワークインターフェイス、
- 8 0 3 制御部、
- 8 1 0 認証用ユーザデータベース、
- 8 1 1 実行アプリケーション

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl' G08G1/137, H04M11/00 302, H04M 3/42, G06F13/00 530, G06F17/60 326

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl' G08G1/137, H04M11/00 302, H04M 3/42, G06F13/00 530, G06F17/60 326

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1926-1996
日本国公開実用新案公報	1971-2001
日本国登録実用新案公報	1994-2001
日本国実用新案登録公報	1996-2001

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 10-255022 A(ソニー株式会社), 25. 9月. 1998(25. 09. 98) 第5頁第8欄第36行—第6頁第9欄第21行、第1図(ファミリーなし)	1-16
Y	JP 11-260045 A(ソニー株式会社), 24. 9月. 1999(24. 09. 99) 第14頁第25欄第30行—同頁第26欄第25行、第10図(ファミリーなし)	1-16
Y	JP 10-330705 A(ソニー株式会社), 18. 12月. 1998(18. 12. 98) 特許請求の範囲の記載、(ファミリーなし)	6-16

 C欄の続きにも文献が列挙されている。 パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」口頭による開示、使用、展示等に言及する文献
 「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」同一パテントファミリー文献

国際調査を完了した日 10. 09. 01	国際調査報告の発送日 18. 09. 01
国際調査機関の名称及びあて先 日本国特許庁 (ISA/J.P) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官 (権限のある職員) 仲村 靖 印 電話番号 03-3581-1101 内線 3314